Prof. Dr. Heinrich Amadeus Wolff, Universität Bayreuth[1]

Die unterschiedlichen Schutzelemente des deutschen und europäischen Datenschutzes

I. Was ist Datenschutz?

Das Datenschutzrecht in Deutschland ist gerade im Umbruch. Bisher hat auf Bundesebene das Bundesdatenschutzgesetz gegolten, das Mai 2018 außer Kraft treten wird (hier abgekürzt BDSG-alt).[2] Das BDSG hat eine alte europäische Richtlinie umgesetzt, die auch im Mai 2018 außer Kraft treten wird (die sogenannte Datenschutzrichtlinie).[3] Ab Mai 2018 wird das neue europäische Recht anwendbar sein. Für die Strafverfolgung und Straftatverhütung im weiteren Sinne wird eine europäische Richtlinie maßgeblich sein,[4] für die sonstige Datenverarbeitung greift die sogenannte Datenschutz-Grundverordnung.[5] Diese Änderungen auf europäischer Ebene haben eine Änderung der deutschen Gesetze erforderlich gemacht. Das neue Bundesdatenschutzgesetz wurde erlassen mit dem Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU) vom 30. Juni 2017.[6]

Datenschutz will die Verarbeitung von personenbezogenen Daten regeln. Personenbezogene Daten sind Einzelangaben über eine bestimmte oder bestimmbare Person.[7] Verarbeitung ist jeder Umgang

---

1 Schriftliche Fassung eines Vortrags, den der Autor im März 2018 an der Chinese Culture University (PCCU) in Taipeh (Taiwan) gehalten hat. Der Aufsatz soll in einer chinesischen Übersetzung in Taiwan erscheinen.

2 Bundesdatenschutzgesetz (BDSG) – s. http://www.gesetze-im-internet.de/bdsg_1990/BJNR029550990.html.

3 Datenschutzrichtlinie (Richtlinie (EG) 95/46 des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr [DSRL]) - http://eur-lex.europa.eu/legal-content/DE-EN/TXT/?uri=CELEX:31995L0046&from=DE.

4 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates.

5 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) s. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&rid=1.

6 BGBl I 2097 - s. https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*[@attr_id='bgbl117s2097.pdf']#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D__1517397588857; s. dazu die Gesetzesmotive BT-Drs. 18/11325 – s. http://dipbt.bundestag.de/doc/btd/18/113/1811325.pdf.

7 § 3 Abs. 1 BDSG-alt (Fn. 2); in gleicher Weise Art. 4 Abs. 1 Datenschutz-Grundverordnung (Fn.4).

mit diesen Daten,[8] insbesondere Erhebung, Speicherung, Löschung, Änderung und Nutzung.[9] Die Art der Daten ist unerheblich. Auch belanglose Daten werden geschützt.[10] Der Grund des Datenschutzes liegt im allgemeinen Persönlichkeitsrecht.[11] Der Datenschutz bildet einen erheblich vorgelagerten Persönlichkeitsschutz. Er greift schon ein, wenn die Persönlichkeit selbst noch nicht gefährdet ist. Anknüpfungspunkt ist allein der Charakter einer Information als personenbezogenes Datum. Wer Daten anderer Personen verarbeiten will, bedarf dafür grundsätzlich eines Rechtsgrundes.[12]

II. Struktur des Datenschutzes

Der Datenschutz erreicht den Schutz auf differenzierendem Wege. Die Differenzierung äußert sich in folgender Struktur. Es gibt einen allgemeinen Datenschutz, der versucht, allgemeine Regeln für jede Art von Verarbeitung aufzustellen. Daneben gibt es eine zweite Ebene, die differenzierende Regelungen aufstellt, um besonderen Situationen, wie etwa Gerichten oder Kirchen, gerecht zu werden. Weiter werden besondere Regelungen für besonders gefährliche Vorgänge aufgestellt. Die dritte Ebene bilden Kontrolle und Sanktionen. Die anschließende vierte Ebene bezweckt den Schutz dieses Systems davor, dass durch den internationalen Datenverkehr der eigene Schutzstandard ausgehebelt wird. Jede dieser vier Ebenen soll im Folgenden kurz angesprochen werden.

III. Die tragenden Prinzipien des Datenschutzes des allgemeinen Schutzes

Der allgemeine Schutz ist am einfachsten zu erkennen, wenn man sich seine tragenden Prinzipien anschaut. Diese sind:

- Verbotsprinzip
- Gebot der Zweckbindung
- Grundsatz der Erforderlichkeit
- Grundsatz der Direkterhebung
- Verbot der Vorratsdatenspeicherung.

---

8 Art. 4 Abs. 2 Datenschutz-Grundverordnung (Fn.4).

9 § 3 Abs. 2 BDSG-alt (Fn. 2).

10 BVerfGE 65, 1, 45 – s. http://www.servat.unibe.ch/dfr/bv065001.html.

11 BVerfGE 65, 1, 41 – s. http://www.servat.unibe.ch/dfr/bv065001.html.

12 § 4 Abs. 1 BDSG-alt (Fn. 2); Art. 7 DSRL (Fn. 2).

1. Das Verbotsprinzip

Das Verarbeiten personenbezogener Daten ist grundsätzlich verboten, es sei denn, der Verarbeiter hat dafür einen Rechtsgrund. Dies gilt auch, wenn ein Privater Daten verarbeitet.[13] Das Verbotsprinzip richtet keinen Schaden an, weil es allgemeine Rechtsgrundlagen gibt, nach denen die Verwaltung all die Daten verarbeiten darf, die sie benötigt, um ihre Aufgaben zu erledigen.[14] Weitere wichtige Rechtsgrundlagen sind:

- die Einwilligung des Betroffenen, die freiwillig, informiert und klar erklärt wird und grundsätzlich widerruflich ist;[15]
- die Berechtigung, Daten zu verarbeiten, um einen Vertrag zu erfüllen oder um eine gesetzliche Pflicht zu erfüllen.[16]
- Wichtig im privaten Bereich ist die Erlaubnis, Daten zu verarbeiten, wenn das Interesse des Verantwortlichen, das Interesse der betroffenen Person überwiegt.[17]

2. Zweckbindung

Der Zweckbindungsgrundsatz ist das Datenschutzprinzip, das den Datenschutz von anderen Rechtsgebieten deutlich trennt. Er gibt dem Datenschutz sein eigenes Gepräge. Der Zweckbindungsgrundsatz besagt: Personenbezogene Daten dürfen nur für den Zweck verwendet werden, für den sie rechtmäßig erhoben wurden.[18] Der Zweck muss vor der Erhebung festgelegt worden sein. Will man die Zweckbindung und die Daten voneinander lösen, benötigt man dafür wiederum eine neue Rechtsgrundlage.[19] Eine Weitergabe der Daten an Dritte ist nur möglich, wenn diese für den Zweck gestattet ist.

3. Grundsatz der Erforderlichkeit

Der Grundsatz der Erforderlichkeit lautet: Eine Datenverarbeitung personenbezogener Daten ist nur zulässig, soweit diese zur Erreichung des Zweckes notwendig ist.[20] Ein Rechtsgrund für eine

---

13 *Bäcker*, in: Wolff/Brink (Hg.), BeckOK-Datenschutzrecht, § 4 BDSG, (22. Edition- Stand: 01.02.2017), Rn. 3 – vgl. https://beck-online.beck.de/?vpath=bibdata\komm\BeckOKDatenS_22\BDSG\cont\BECKOKDATENS.BDSG.P4.glA.glI.htm (kostenpflichtiger Zugang).

14 §§ 13, 14 BDSG-alt (Fn. 2); Art. 6 Abs. 1 UAbs. 1 lit. e) Datenschutz-Grundverordnung (Fn.4); § 3 BDSG-neu (Fn. 6).

15 §§ 4, 4a BDSG-alt (Fn. 2); Art. 6 Abs. 1 UAbs. 1 lit. a), Art. 7, 8 Datenschutz-Grundverordnung (Fn.4).

16 § 28 Abs. 1 Nr. 1 BDSG-alt (Fn. 2); Art. 6 Abs. 1 UAbs. 1 lit. b) Datenschutz-Grundverordnung (Fn.4).

17 § 28 Abs. 1 Nr. 2 BDSG-alt (Fn. 2); Art. 6 Abs. 1 UAbs. 1 lit. f) Datenschutz-Grundverordnung (Fn.4).

18 Art. 5 Abs. 1 lit. b) Datenschutz-Grundverordnung (Fn.4).

19 Art. 6 Abs. 4 Datenschutz-Grundverordnung (Fn.4).

20 Art. 6 Abs. 1 Datenschutz-Grundverordnung (Fn.4); *Wolff*, in: Schantz/Wolff, Das neue Datenschutzrecht, 2017, Rn. 428 ff. s. https://beck-

Verarbeitung erlaubt nicht, dass alle Daten herangezogen werden, die nützlich sein können, sondern nur die Daten, die konkret geboten sind, zur Erreichung eines konkret festgelegten Zweckes.[21]

Ein Sonderfall des Gebots der Erforderlichkeit bildet das Verbot der Vorratsdatenspeicherung. Es besagt: Die Erhebung von Daten, ohne dass die Daten für einen konkreten Zweck benötigt werden, ist grundsätzlich unzulässig.[22] Eine selbständige Ausprägung bildet dabei das Verbotder anlassbezogenen Datenerhebung. In den Fallkonstellationen, in denen unklar ist, wie viele Daten die verarbeitende Stelle für die Zweckerreichung benötigt, muss sie erst einmal so viele Daten erheben wie sie benötigt, um die erste anstehende Aufgabe zu bewältigen, und darf erst dann, wenn sie nun sieht, dass sie weitere Daten benötigt, weitere Daten für die Erreichung der zweiten Stufe erheben.

4. Grundsatz der Direkterhebung

Der Grundsatz der Direkterhebung lautet: Personenbezogene Daten sind grundsätzlich beim Betroffenen zu erheben. Eine Erhebung in anderer Weise bedarf einer sachlichen Rechtfertigung.[23] Der Grundsatz ist nicht sehr streng umgesetzt. Der Grundsatz ist aber der sachliche Grund dafür, dass man die betroffene Person grundsätzlich informieren muss, wenn man Daten über sie bei Dritten erhebt.

IV. Das Prinzip der Schutzbereichsräume am Beispiel der Gesundheitsdaten

1. Ausgeklammerte Bereich

Auf diesen allgemeinen Datenschutz setzten Normen auf, die besondere Datenschutzbereiche schaffen.[24] Ein Teil dieser Datenschutzräume ergibt sich aus der Natur der Sache, teilweise werden sie vom Gesetzgeber bestimmt. So gilt das einfache Datenschutzrecht etwa nicht in folgenden Räumen:

- Keine Datenschutzregelung gibt es für eine Verarbeitung, die alleine im menschliche Gehirn abläuft.

---

online.beck.de/?vpath=bibdata/komm/SchantzWolffHdbNeuDSR_1/cont/SchantzWolffHdbNeuDSR%2Ehtm (kostenpflichtiger Zugang).

21 EuGH Urt. v. 16. 12. 2008, Rs. C-524/06 – Huber: Ausländerzentralregister, Rn. 47.

22 BVerfGE 125, 260 (317), s. http://sorminiserv.unibe.ch:8080/tools/ainfo.exe?Command=ShowPrintVersion&Name=bv125260.

23 § 4 Abs. 2 BDSG-alt (Fn. 2); *Wolff*, in: Schantz/Wolff (Fn. 20), Datenschutzrecht, 2017, Rn. 456 ff.; s.a. Art. 11 Datenschutz-Grundverordnung (Fn.4).

24 *Wolff*, in: Wolff/Brink (Fn. 13)(Hg.), Prinzipien des Datenschutzrechts, Rn. 2; *Wolff*, in: Schantz/Wolff (Fn. 20), Datenschutzrecht, 2017, Rn. 451 ff.

- Vom einfachen Recht geschützt sind nur die Daten von natürlichen Personen. Die Daten von juristischen Personen fallen nicht unter das einfache Datenschutzrecht.[25] Juristische Personen sind danach nur dann geschützt, wenn die relevanten Daten die dahinterstehenden natürlichen Personen betreffen. Dies ist etwa möglich, wenn der Name der juristischen Person zugleich (teilweise) auch der Name einer natürlichen Person ist.[26]
- Frei vom spezifischen Datenschutz ist die Datenverarbeitung durch Private allein zu privaten Zwecken.[27]

2. Unterschiedliche Rechtsregime

Es gibt gewisse Unterschiede, die darauf beruhen, dass in Deutschland nicht nur ein Gesetzgeber für das gesamte Datenschutzrecht zuständig ist, sondern drei: Der Verordnungsgeber der Europäischen Union, der Gesetzgeber auf der Ebene des Gesamtstaates Deutschland und der Gesetzgeber auf der Ebene der Gliedstaaten. Diese Differenzierungen beruhen nicht auf der Natur des Datenschutzes, sondern allein auf der Kompetenzlage und unterschiedlichen Schwerpunktsetzungen der einzelnen Gesetze. Aufgrund der Kompetenzverteilung zwischen Europa und Deutschland gibt es drei Regelungsräume: den Bereich der Verarbeitung zur Straftatenverfolgung und Straftatenverhütung,[28] den allgemeinen europäischen Bereich[29] und den rein nationalen Bereich,[30] der nur von den Mitgliedsstaaten geregelt wird und schwer zu bestimmen ist. Dazu gehören zumindest: Datenverarbeitung zu militärischen Zwecken, Datenverarbeitung der Nachrichtendienste/Geheimdienste, Datenverarbeitung für Begnadigungen, Datenverarbeitung für Orden und Ehrenbürgerverleihungen. Der Bereich, den Deutschland regeln darf, wird dann wiederum auf Bund und Land verteilt. Dabei regelt der Bund die Datenverarbeitung durch Private und durch Bundesbehörden und die Länder die Datenverarbeitung durch Landesbehörden.

3. Privilegierte Bereiche

Weiter gibt es bestimmte Sachbereiche, in denen die allgemeinen Regeln etwas abgeschwächt werden. So kennt das Datenschutzrecht Sondergebiete, in denen die Datenverarbeitung abweichend von den allgemeinen Regeln vorgenommen werden kann. Die Abweichungen bestehen teilweise darin, dass das Europarecht den Mitgliedstaaten gestattet, Sonderregelungen zu erlassen: Bereiche,

---

25 S. Fn. 7.

26 EuGH (Große Kammer), Urt. v. 9. 11. 2010, Rs. C-92/09 und C-93/09 – Volker und Markus Schecke GbR und Hartmut Eifert/Land Hessen, Rn. 53.

27 Art. 2 Abs. 2 lit. c) Datenschutz-Grundverordnung (Fn.4).

28 §§ 1-21 und §§ 45-84 BDSG-neu.

29 Art. 2 Datenschutz-Grundverordnung (Fn.4) i.V.m. §§ 1-43 BDSG-neu (Fn. 6).

30 § 85 BDSG-neu i.V.m. § 1 Abs. 8 BDSG-neu (Fn. 6).

in denen das der Fall ist, sind: Datenschutz für Beschäftigte,[31] Datenschutz in der Wissenschaft, im Archivwesens, in der Statistik,[32] beim Recht der nationalen Kennziffern[33] und für Berufe mit Geheimhaltungspflichten.[34] Auch für die Gerichte gibt es Sonderregelungen.[35] Früher waren die Gerichte, sofern sie Recht sprachen, vollständig vom einfachen Datenschutzrecht befreit und mussten sich nur an den verfassungsrechtlichen Datenschutz halten.[36] Im neuen europäischen Datenschutzrecht ist dies nun anders. Danach gilt das allgemeine Datenschutzrecht auch für die Gerichte bei der Rechtsprechung,[37] jedoch mit einer Erleichterung im Bereich der sensiblen Daten, um so das Gerichtsverfahren zu ermöglichen.[38] Zudem sind die Gerichte im Bereich der Rechtsprechung freigestellt von der Aufsicht durch die Aufsichtsbehörden.[39] Üben die Gerichte Verwaltungstätigkeit aus, sind sie allerdings wiederum der Aufsicht unterstellt. Daneben gibt es Bereiche, bei denen nicht eine andere staatliche Ebene berechtigt wird, Abweichendes zu regeln, sondern die betroffenen Kreise eigene Regeln erlassen dürfen. So ist dies im Ergebnis im Presserecht und bei den Kirchen.[40]

4. Verschärfungen für bestimmte Verarbeitungen

a) Folgenabschätzung für gefährliche Datenverarbeitungen

So wie es Privilegierungen gibt, gibt es umgekehrt auch Verschärfungen. Das Datenschutzrecht unterscheidet verschiedene Standards je nach Art der Daten und je nach Art der Verarbeitung. Das europäische Datenschutzrecht kennt Pflichten, bei einer Verarbeitung von Daten, die für den Betroffenen besonders gefährlich ist. Gefährlich ist sie, wenn die Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Bei dieser gefährlichen Datenverarbeitung muss der Betroffene, bevor er die Verarbeitung aufnimmt, eine Folgenabschätzung vornehmen, die die Gefahr in den Blick nimmt und versucht, diese einzudämmen und Schutzmechanismen zu installieren.[41] Die

---

31 Art. 88 Datenschutz-Grundverordnung (Fn.4).

32 Art. 5 und Art. 89 Datenschutz-Grundverordnung (Fn.4).

33 Art. 87 Datenschutz-Grundverordnung (Fn.4).

34 Art. 90 Datenschutz-Grundverordnung (Fn.4).

35 Art. 55 Abs. 3, Art. 37 Abs.1 lit. a) Datenschutz-Grundverordnung (Fn.4).

36 § 1 Abs. 2 Nr. 2 b BDSG-alt (Fn. 2).

37 § 1 Abs. 1 BDSG-neu (Fn. 6).

38 Art. 9 Abs. 2 lit f) Datenschutz-Grundverordnung (Fn.4).

39 Art. 55 Abs. 3, Art. 37 Abs.1 lit. a) Datenschutz-Grundverordnung (Fn.4).

40 Art. 85 und Art. 91 Datenschutz-Grundverordnung (Fn.4).

41 Art. 35 Datenschutz-Grundverordnung (Fn.4).

Folgenabschätzung enthält insbesondere eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen. Weiter enthält sie eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck. Schließlich ist eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen sowie die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt wird, aufzunehmen. Es ist der Nachweis dafür zu erbringen, dass die Datenschutz-Grundverordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung zu tragen ist.

b) Verarbeitung sensibler Daten am Beispiel der Gesundheitsdaten

Von der auf die Gefährlichkeit der Art der Verarbeitung bezogenen Differenzierung zu unterscheiden ist die Differenzierung, die an die Art der Daten anknüpft. Die Datenschutz-Grundverordnung kennt zwei Arten von Daten: die normalen personenbezogenen Daten, unter die zum Beispiel auch der Name fällt, und besonders sensible Daten, die in Art. 9 Datenschutz-Grundverordnung definiert sind und die mit dem etwas schwerfälligen Begriff "besondere Kategorien personenbezogener Daten“ bezeichnet werden. Zu diesen besonders sensiblen Daten gehören etwa Gesundheitsdaten und genetische Daten. Gesundheitsdaten sind personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.[42]

Gesundheitsdaten spielen im Datenschutz eine besondere Rolle. Sie führen zu besonders sensible Verarbeitungsvorgänge. Bei Ihnen greifen nicht die allgemeinen Erlaubnistatbestände für eine Verarbeitung. Vielmehr müssen spezielle Rechtfertigungsgründe vorliegen. Eine Rechtfertigung ist zunächst die Einwilligung.[43] Die Einwilligung in die Verarbeitung von Gesundheitsdaten unterscheidet sich von der Einwilligung in die übrige Datenverarbeitung durch zwei Gesichtspunkte, zum einen muss sie sich besonders klar auf die Kategorie der Gesundheitsdaten beziehen und zum anderen darf die Zweckbestimmung bei den Gesundheitsdaten weiter sein als bei anderen Verarbeitungen, weil auf diese Weise die wissenschaftliche Forschung privilegiert werden sollen. Fehlt es an einer Einwilligung, ist eine Rechtfertigung trotzdem möglich bei folgenden Fallgestaltungen:

- zu Abrechnungszwecken für einen Arzt oder eine Krankenhaus;[44]

---

42 Art. 4 Abs. 5 Datenschutz-Grundverordnung (Fn.4).

43 Art. 9 Abs. 2 lit. a) Datenschutz-Grundverordnung (Fn.4).

44 Art. 9 Abs. 2 lit. f) Datenschutz-Grundverordnung (Fn.4).

- zu Verarbeitung zwecks Ausübung von Rechten, die aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit erwachsen;[45]
- zu Behandlungszwecken durch medizinisches Personal; [46]
- zum Zwecke der Gesundheitspolitik, wobei die Gewährleistung von Berufsgeheimnissen zu beachten ist; [47]
- zu Forschungszwecken.[48]

Liegt einer dieser fünf Ausnahmetatbestände vor, hat dies aber nicht zur Folge, dass die Gesundheitsdaten schutzlos wären. Auch bei dem Rückgriff auf diese Ausnahmefälle verlangt das europäische Datenschutzrecht ausdrückliche Regelungen des nationalen Rechts, um diese Ausnahmetatbestände einzuhegen und Sicherheiten vor einer zu weitgehenden Verarbeitung zu geben. Das nationale Recht muss ausreichende Sicherheiten für die Daten vorsehen. Sicherheiten in diesem Sinne sind dabei:

- die Anonymisierung, sofern sie möglich ist;
- die Pseudonymisierung; dort wo sie möglich ist, mit der Pflicht der Protokollierung von Zugriffen auf den Datenschlüssel;
- ein hoher Standard der Datensicherheit; die möglichst sichere Speicherung der Daten;
- Einschränkung der Weitergabemöglichkeiten.

Eine besondere Rolle misst die DS-GVO insbesondere der Forschung und somit auch der Forschung an Gesundheitsdaten zu. Die Forschung wird von der DS-GVO in zweifacher Hinsicht privilegiert. Zum einen gestattet die Verordnung die Einschränkung der Rechte der Betroffenen bei Verarbeitung zu Wissenschaftszwecken in größerem Umfang als normalerweise. Zum anderen enthält die Regelung einen ausdrücklichen Hinweis darauf, dass bei der Verarbeitung zu Forschungszwecken die Regelungen zur Zweckentfremdung in Art. 6 Abs. 4 DS-GVO) nicht unmittelbar gilt.[49] Dies ermöglicht, die Medizinforschung sinnvoll fortzusetzen.

V. Die dritte Ebene: Die Absicherung durch Sanktion und Kontrolle

1. Allgemein

Die Einhaltung des Datenschutzes kann die Produktion der Wirtschaft erschweren und den Produktionsprozess verteuern, weshalb sowohl die Wirtschaft als auch die Nationalstaaten Interesse

---

45 Art. 9 Abs. 2 lit. b) Datenschutz-Grundverordnung (Fn.4).

46 Art. 9 Abs. 2 lit. h) Datenschutz-Grundverordnung (Fn.4).

47 Art 9 Abs. 2 lit. i) Datenschutz-Grundverordnung (Fn.4).

48 Art. 89 Datenschutz-Grundverordnung (Fn.4).

49 Art. 5 Datenschutz-Grundverordnung (Fn.4).

daran haben können, die Einhaltung des Datenschutzes nicht zu ernst zu nehmen. Das europäische Datenschutzrecht sieht dieses Problem und versucht, durch institutionelle Garantien die Einhaltung der Datenschutznormen zu ermöglichen. Zu diesen Sicherstellungen gehören die Instrumente

- Rechte der Betroffenen (Lösung, Sperrung, Auskunft, Widerspruch) und Ansprüche, insbesondere Schadensersatzansprüche;
- wirkungsvolle Sanktionen bei Verstößen gegen den Datenschutz, insbesondere Ordnungswidrigkeitensanktionen, die aus dem Wettbewerbsrecht bekannt sind und enorm hoch sind (bis 4 % des Weltumsatzes des betroffenen Unternehmens);
- eine effiziente und unabhängige Aufsicht durch die Aufsichtsbehörden, auf die noch kurz eingegangen werden soll.

2. Die Aufsichtsbehörden

a) Die Stellung

Für die Kontrolle des Datenschutzrechtes sieht das Europarecht besondere Behörden vor, die früher Kontrollstellen hießen[50] und nun Aufsichtsbehörden[51] genannt werden. Ihre Stellung ist im europäischen Recht ausführlich geregelt. Es wird zwischen Aufgaben und Befugnissen getrennt. Das europäischen Recht führt 21 Aufgaben der Aufsichtsbehörden auf, dazu gehören jeweils festgelegte Überwachungs-, Durchsetzungs-, Beratungs- und Unterstützungstätigkeiten in folgenden Bereichen: Überwachung aller Normen der DS-GVO; Sensibilisierung und Aufklärung der Öffentlichkeit; Beratungstätigkeit öffentlicher Stellen, Beratung von Verantwortlichen, Auftragsverarbeitern und Betroffenen; Rechtsdurchsetzung betroffener Personen; Zusammenarbeit mit anderen Aufsichtsbehörden; Verfolgung datenschutzrechtsrelevanter Entwicklungen; Festlegung von Standardvertragsklauseln, Aufstellung eines internen Verzeichnisse über Datenschutzverstöße und die Abhilfemaßnahme.[52] Besonders deutlich wird das weite Aufgabenfeld der Aufsichtsbehörde etwa an Art. 57 Abs. 1 lit. v DS-GVO, wonach zu den Aufgaben gehört, „jede sonstige Aufgabe im Zusammenhang mit dem Schutz personenbezogener Daten [zu] erfüllen."

Die Befugnisse der Aufsichtsbehörden sind ebenfalls sehr umfangreicht. Sie werden in drei Gruppen eingeteilt, und zwar Untersuchungsbefugnisse, Abhilfebefugnisse und Genehmigungsbefugnisse.[53] Wichtig ist, dass die Aufsichtsbehörden, die einzigen sind, die Geldbußen wegen Verletzung des

---

50 Art. 28 DSRL (Fn.3).

51 Art. 51 Datenschutz-Grundverordnung (Fn.4).

52 Art. 57 Datenschutz-Grundverordnung (Fn.4).

53 Art. 58 Datenschutz-Grundverordnung (Fn.4).

Datenschutzrechts verhängen dürfen[54] und die zudem die Aufgabe haben, einen Beitrag zur einheitlichen Anwendung der Datenschutz-Grundverordnung in der gesamten Union zu leisten und das Datenschutzrecht zu konkretisieren.[55]

Die Aufsichtsbehörden haben dabei eine besondere Stellung. Sie besitzen eine außergewöhnliche und umfassende Unabhängigkeit. Gem. Art. 52 Abs. 1 DS-GVO handelt jede Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben und bei der Ausübung ihrer Befugnisse völlig unabhängig. Unabhängigkeit bedeutet zunächst, dass die Leiter und das Personal der Aufsichtsbehörden bei der Erfüllung ihrer Aufgaben und der Ausübung ihrer Befugnisse gemäß der Datenschutz-Grundverordnung weder direkter noch indirekter Beeinflussung von außen unterliegen; sie ersuchen weder um Weisung noch nehmen sie Weisungen entgegen. Unzulässig ist die Aufsicht in der Form der Rechts- und Fachaufsicht, das heißt jeglicher Einflussnahme, Weisungen, Anordnungen, Änderungsbegehren, Aufhebungsbegehren oder Ersetzungsbegehren. Unzulässig ist auch eine Dienstaufsicht, die der im Beamtenrecht üblichen entspricht. Diese Unabhängigkeit schließt nicht nur jegliche Einflussnahme seitens der kontrollierten Stellen aus, sondern auch jede Anordnung und jede sonstige äußere Einflussnahme, sei sie unmittelbar oder mittelbar, durch die in Frage gestellt werden könnte, dass die genannten Kontrollstellen ihre Aufgabe, den Schutz des Rechts auf Privatsphäre und den freien Verkehr personenbezogener Daten ins Gleichgewicht zu bringen, erfüllen. Das bedingt, dass die für den Schutz personenbezogener Daten zuständigen Aufsichtsbehörden mit einer Unabhängigkeit ausgestattet sein müssen, die es ihnen ermöglicht, ihre Aufgaben ohne äußere Einflussnahme wahrzunehmen. Dabei reicht der Umstand, dass eine solche Aufsichtsbehörde insofern funktionell unabhängig ist, als ihre Mitglieder in Ausübung ihres Amtes unabhängig und an keine Weisungen gebunden sind, für sich allein nicht aus, um diese Aufsichtsbehörde vor jeder äußeren Einflussnahme zu bewahren. Der EuGH sprach einmal, etwas theatralisch und wohl über das Ziel hinausschießend, von den „Hütern der Grundrechte“[56].

b) Kritik

Die Aufsichtsbehörden besitzen einen erheblichen Einfluss in Deutschland und Europa und dienen einer effektiven Durchsetzung des Datenschutzes. Der Datenschutz wäre in Europa viel schlechter, wenn es diese Behörden nicht gäbe. Dennoch ist die Konstruktion nicht besonders glücklich aus folgenden Gründen:

---

54 Art. 83 Datenschutz-Grundverordnung (Fn.4).

55 Art. 51 Abs. 2 Datenschutz-Grundverordnung (Fn.4).

56 EuGH Urt. v. 14,10.2008, Rs. C-518/07 (Kommission/Deutschland) [Aufsichtsbehörde] Rn. 22 f.

aa) Die sachliche Unabhängigkeit als inadäquates Strukturprinzip

Die Unabhängigkeit bei der Kontrolle von Privaten bei der Verarbeitung weicht ohne ausreichende sachliche Legitimation in erheblicher Weise von einem in Deutschland bewährtem Organisationsrecht ab. Eigentlich darf in Deutschland nur eine Stelle Hoheitsausübung ausüben, die vom Parlament kontrolliert werden kann. Wir sprechen von demokratischer Legitimation.[57] Die organisatorische Sonderrolle, die den Aufsichtsbehörden durch die Unabhängigkeit auch im privaten Bereich zugewiesen wird, ist danach nicht gerechtfertigt. Da sie auf Europarecht beruht, ist sie wirksam und zu beachten, sie ist aber aus deutscher Sicht sachlich dennoch nicht angemessen.

bb) Administrative Überforderung

Die strenge Unabhängigkeit, die den Aufsichtsbehörden zugewiesen wird, führt dazu, dass die Aufsichtsbehörden vieles alleine machen müssen, wofür sie eigentlich zu klein sind. So ist etwa der Bedarf an Fremdsprachenkompetenzen innerhalb einer Aufsichtsbehörde aufgrund der Vernetzung mit den anderen europäischen Aufsichtsbehörden beachtlich, die Möglichkeiten, diesen Bedarf zu decken, gering.

cc) Unvereinbare Rolle von Berater und Aufsicht

Die Aufsichtsbehörden besitzen Aufgaben, die in sich spannungsvoll sind. Die Aufsichtsbehörden werden konstruiert als Helfer der betroffenen Personen, als Berater der Verantwortlichen und gleichzeitig als Kontrolleure. Dies mag nicht so schlimm klingen, aber nur auf den ersten Blick.

Die Aufsichtsbehörde soll den Verantwortlichen in vielfältiger Form beraten. Außerdem hat jede betroffene Person das Recht, sich an ihre Aufsichtsbehörde zu wenden,[58] unabhängig davon, ob diese zuständig ist oder nicht. Die Aufsichtsbehörde ist dann verpflichtet auf diese Beschwerde sachlich zu reagieren. Die Aufsichtsbehörde soll hinwirken auf den Erlass von Verhaltensvorschriften, auf die Zertifizierung; sie soll beraten bei der Einhaltung der technischen Vorschriften und der Folgenabschätzung. Ihr gegenüber müssen erhebliche Verstöße gemeldet werden.

Gleichzeitig ist sie aber die Behörde, die erhebliche Ordnungswidrigkeitensanktionen erlassen und Abhilfemaßnahme zwangsweise durchsetzen kann.[59] Das ist eine spannungsvolle Beratung, wenn der Berater die Möglichkeit hat, seinen Willen mit staatlicher Gewalt durchzusetzen.

Weiter sind die Vorgaben der Datenschutz-Grundverordnung enorm vage – wer die Interpretationsherrschaft über diese Vorschriften hat, besitzt faktisch die Macht festzulegen, was gilt.

---

57 BVerfGE 83, 60 (73) s. http://sorminiserv.unibe.ch:8080/tools/ainfo.exe?Command=ShowPrintVersion&Name=bv093037; BVerfGE 93, 37 (67 ff.); BVerfGE 107, 59 (92 ff.); BVerfGE 111, 191 (216 ff.) s. http://www.servat.unibe.ch/dfr/bv111191.html.

58 Art. 77 Datenschutz-Grundverordnung (Fn.4).

59 Art. 83 Datenschutz-Grundverordnung (Fn.4).

Die Interpretationsherrschaft liegt nach der Konstruktion der Verordnung formal letztendlich beim EuGH, vorgelagert beim Europäischen Datenschutzausschuss, der sich aus den einzelnen Aufsichtsbehörden zusammensetzt,[60] im Alltag aber bei den Aufsichtsbehörden, gemildert durch die gerichtliche Kontrolle.

Dies alles führt dazu, dass der Betroffene die Rechtssicherheit nicht durch die Auslegung des objektiven Rechtes erhält, sondern durch die Zusagen der Aufsichtsbehörden. Nicht die Norm, sondern das Wort der Aufsichtsbehörde ist maßgeblich. Dies wird kaum gut gehen können. Der Rechtsstaat lebt von der Kraft der Norm und nicht von der Kraft des Wortes der zuständigen Behörde. Da Recht wird zur Verhandlungssache und gilt nicht mehr objektiv.

dd) Problem der Anwendung fremden Rechts

In besonderen Konstellationen kann die Aufsichtsbehörde verpflichtet sein, ausländisches Recht anzuwenden.[61] Da kennt sie aber in aller Regel nicht.

VI. Der Schutz vor der Übermittlung ins Ausland

Der beste Datenschutz in Europa nützt nichts, wenn die Daten ins Ausland verbracht werden können und dort dann ohne Beachtung des Datenschutzes verarbeitet werden können. Daher regelt das Datenschutzrecht die Verbringung der Daten in Drittstaaten und lässt diese im Ausgangspunkt erst einmal nicht zu.[62] Verbringung in diesem Sinne ist jede Offenlegung personenbezogener Daten gegenüber Empfängern in Drittstaaten.[63] Erfasst sind auch Fälle, in denen die Daten an einen unselbständigen Unternehmensteil oder einen Auftragsverarbeiter in einem Drittstaat übermittelt werden oder die Daten vom Verantwortlichem mit Sitz in einem Drittstaat direkt beim Betroffenen erhoben werden und dort erstmals durch einen Verantwortlichen verarbeitet werden. Eine Sonderstellung im Kontext der Drittstaatenübermittlung nehmen bisher Veröffentlichungen auf Websites ein. Der EuGH hat entschieden, die Veröffentlichung von Daten auf einer Website, deren Hostprovider Server in der EU nutzt, sei keine Drittstaatenübermittlung.[64]

---

60 Art. 68 ff. Datenschutz-Grundverordnung (Fn.4).

61 Beispiel: Verkauft beispielsweise ein Unternehmen mit alleinigem Sitz in Polen in Deutschland Waren in einer Weise, die nicht als grenzüberschreitende Verarbeitung zu verstehen ist und nimmt es Ausnahmen in Anspruch, die Polen im Rahmen einer Öffnungsklausel rechtmäßig national normiert hat, ist die deutsche Aufsichtsbehörde zuständig, aber verpflichtet, das fremde Recht anzuwenden.

62 Art. 44 Datenschutz-Grundverordnung (Fn.4).

63 *Schantz*, in: Schantz/Wolff (Fn. 20), Datenschutzrecht, 2017, Rn. 757.

64 EuGH Urt. v. 6. 11. 2003, Rs. C-101/01 – Bodil Lindquist, Rn. 70 f.

Eine Verbringung ist zunächst zulässig, wenn der Drittstaat ein Datenschutzniveau aufweist, das mit dem europäischen vergleichbar ist. Darüber entscheidet die Kommission.[65] Fehlt es an der Angemessenheit des gesamten Datenschutzes, ist die Verbringung zulässig, wenn der Empfänger selbst ein angemessenes Schutzniveau sicherstellen kann, durch eigene Regeln, durch Verträge oder Vergleichbares.[66] Ist dies nicht möglich, kann die Verbringung dennoch zulässig sein, sofern einer der ausdrücklich normierten Ausnahmefälle vorliegt.[67] Diese Ausnahmefälle sind etwa: Vorliegen einer Einwilligung nach Aufklärung; die Übermittlung ist für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich. Eine Ausnahme bildet auch die Übermittlung zum Zweck eines Vertragsschlusses zugunsten eines Dritten ebenso wie die Übermittlung zum Schutz lebenswichtiger Interessen der betroffenen Person. Schließlich bleibt eine Übermittlung möglich, die aus wichtigen Gründen des öffentlichen Interesses notwendig ist. Kommen die Daten aus einem öffentlichen Register, ist die Übermittlung auch zulässig.

VII. Schluss

Das Datenschutzrecht versucht, zum einen durch ein Schutzsystem mit mehreren Ebenen einen effektiven Schutz wirksam werden zu lassen und zum anderen adäquate Lösungen für die jeweils relevante Situation anzubieten. Bei der Konstruktion der Aufsichtsbehörde ist das Recht etwas weiter gegangen, als notwendig gewesen wäre.

---

65 Art. 45 Datenschutz-Grundverordnung (Fn.4).

66 Art. 46 - Art. 48 Datenschutz-Grundverordnung (Fn.4).

67 Art. 49 Datenschutz-Grundverordnung (Fn.4).